IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application for:

First Named Inventor: REISMAN

Art Unit: 2137

Appln. No.: 09/435,736

Examiner: M. NGUYEN

For: ENCRYPTED AND NON-ENCRYPTED COMMUNICATION OF MESSAGE DATA

Confirmation No.: 5609

SECOND PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The outstanding Office Action rejects groupings of the claims under various combinations of Saliba, Ice, Treka, and Schneier.

The Office Action further objects to claims 2-4, 6, 13, 16-18, 20, 23, 26, 30 and 34. Appellants agree with the Examiner's interpretation of these claims and for purposes of this Appeal would like those claims interpreted consistent with ¶ 4 of the March 23, 2007 Office Action. However, Appellants believe claims 28-29 are in full compliance with 35 U.S.C. §101.

Independent Claim 36 is directed toward a method of communication of data between a first computing device and a second computing device, comprising, *inter alia*, the program on the first computing device receiving a message from the user, wherein the message comprises at least a first and second datum input by the user into the at least first and second input fields, respectively, of the Web page, wherein the first datum is confidential to the user and the second datum is non-confidential to the user, and wherein the first datum comprises at least one of a credit card number and a social security number, the program identifying that the first datum is confidential and the second datum is non-confidential, the first computing device communicating, to the second computing device over an untrusted network, the first datum with encryption and first computing device communicating, to the second computing

device over the untrusted network, the second datum without encryption, wherein the communicating steps occur at least substantially simultaneously.

Independent Claim 40 is directed toward a comparable means, and Independent Claim 44 recites, *inter alia*, a program determining which of the at least first and second user input fields contains confidential information, wherein the first datum is confidential to the user and the second datum is not confidential to the user, the first computing device communicating the first datum to a second computing device over an untrusted network with encryption of the first datum and the first computing device communicating the second datum over the untrusted network to the second computing device without encryption of the second datum.

Independent Claim 45 recites, *inter alia*, a procedure operable to identify that the first datum is confidential and the second datum is non-confidential, wherein a second communication device is in communication with the first communication device and wherein the first computing device communicates, to the second computing device over the untrusted network, the first datum with encryption and the second datum without encryption.

As discussed in the specification, the entry (input) fields allow a user to input characters or text. These entry (input) fields are portions of a web page that can include, for example, a number of entry fields and a number of presentation fields. (See, for example, pgs. 7 and 8 of Appellants specification.)

Appellants respectfully submit the Office has failed to meet the minimum requirements to uphold either a rejection asserting anticipation or *a prima facie* case of obviousness in that at least two features of the independent claims are neither taught nor suggested by any of the references of record.

First, the independent claims include either a program, means, or procedure that identifies that the first datum is confidential and the second datum is non-confidential. While the Office Action points to col. 7, lines 5-8 of Saliba for this teaching, Appellants respectfully submit there is absolutely no teaching or suggestion in this portion, nor in any other portion of Saliba, that teaches the claimed feature. Specifically, the relied upon portion of Saliba merely speaks to specialized functions in the context of electronic shopping. The relied upon portion of Salida states:

> ...(iii) storing, encrypting and forwarding to the merchants payment (e.g., credit card) information, (iv) storing and providing to merchants address information for the shipping of goods, and (v) passing receipts for online purchases to an online banking application such as Microsoft Money.TM. or Quicken.RTM..

Neither this portion, nor any other portion of Slaiba, make any reference whatsoever to functionality nor componentry that is capable of performing the claimed feature.

Secondly, the independent claims are directed toward communicating the information based on the identification such that, for example, the first datum is communicated with encryption and the second datum is communicated without encryption.

The Office Action references Col. 1, lines 33-38, as well as columns 4 and 7, for this teaching. One of the identified portions Saliba states: "These hypertext documents, which are created using HTML (the Hypertext Markup Language), contain the various product offerings and other purchase-related information of the respective merchants, and typically include forms for allowing consumers to return payment and address information to the merchants. One significant problem with this approach is that the existing World Wide Web components (e.g., HTTP, HTML, and existing standard Web browsers) are not well suited for performing general purpose client-server transactions over the Internet, making it difficult to migrate commerce-related functionality to the client (consumer) side." Column 4 discusses common definitions of the internet, client-server, etc, and the relied upon portion of column 7 is reproduced above.

Saliba makes no mention nor provides any functionality or componentry in either these sections nor any other section that anticipates or renders obvious the claimed feature.

Moreover, and in contrast to and teaching away from the claimed invention, Saliba actually specifically states "Because *all information is passed using standard HTTP messages*, end users can access the electronic commerce system from behind Internet firewalls that permit the passage of HTTP traffic." (Emphasis Added)

Additionally, Saliba is addressing an entirely different problem than the claimed invention. As discussed, for example, in Appellants specification, flagged portions of web pages are encrypted while same portion of the same web page are not encrypted, or vice versa. In complete contrast, Saliba address:

> ...the problem of performing commerce-related transactions over the Internet involves the use of specialized client and server software components which communicate with one-another using some transport protocol other than HTTP. This approach, which is used by the version 1.0 electronic commerce system of eShop Inc., generally requires the use of some dedicated TCP/IP port other than port 80, which is reserved for HTTP. (TCP/IP is a low level Internet communications protocol which uses port definitions to route messages to applications.) Unfortunately, many company networks have Internet firewalls (i.e., systems which restrict traffic into and/or out of the company network to provide network security) which block traffic on TCP/IP ports other than port 80 (and possibly a few other reserved ports), preventing consumers from using such electronic commerce systems from their computers at work. Additionally, systems of this type do not take advantage of the widespread use by potential consumers of the World Wide Web.

At least based on these differences, claims 4-5, 10-11, 18-19, 23-24, 26-30, 32-35 and 44-45 are patentably distinguishable from Saliba.

Ice is relied upon to teach steps "d" and "e". Ice is directed toward routing of a transaction card together with a serial number of an encryption unit. Ice States: "at this point, the data transferred from the personal computer 14 the payment server 34 includes both encrypted information identifying the credit card number and unencrypted information specifying the serial number of the encryption unit 26 and the address to which the transaction is to be billed."

The credit card number of Ice is however *not* a user input field in that *the payment server* 34 generates the single-use credit card number and moreover, it is unclear where the Office finds support for these steps occurring "substantially simultaneously" as asserted in that Ice merely discloses transferring information.

In that the remaining references, taken either alone or in combination, fail to overcome the deficiencies noted above, Appellants respectfully submit that all claims are patentably distinguishable from the cited references.

The dependent claims are even further patentably distinct from the cited art.

By way of example, claim 2 recites the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum to include the step of communicating the first datum with encryption and the second datum without encryption in a same packet that comprises the message. *See also* Claims 16, 37, and 42.

This feature is neither suggested nor disclosed by the cited references.

Dependent claim 3 recites the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum to include the steps of communicating the first datum with encryption in a first packet of the message and communicating the second datum without encryption in a second packet of the message different from the first packet of the message. *See also* Claim 17.

This feature is neither suggested nor disclosed by the cited references.

Dependent claim 4 recites the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum comprise the step of employing a same path between the first computing device and the second computing device to communicate the

first datum with encryption and the second datum without encryption. *See also* Claims 18, 38 and 43.

This feature is neither suggested nor disclosed by the cited references.

Dependent claim 5 recites the step of employing the same path to communicate the first datum with encryption and the second datum without encryption to include the step of employing a TCP/IP passage between the first computing device and the second computing device to communicate the first datum with encryption and the second datum without encryption. *See also* Claim 19.

This feature is neither suggested nor disclosed by the cited references.

Dependent claim 6 recites the step of communicating the first datum of the message with encryption of the first datum to include the step of employing a key to encrypt the first datum of the message for communication of the first datum from the first computing device to the second computing device with encryption of the first datum. *See also* Claims 7-9 and 20-22.

This feature is neither suggested nor disclosed by the cited references.

Dependent claim 10 recites the Web page to include hypertext markup language, the first datum to include the credit card number, the second datum to include information related to a purchase by the user and the program to be embedded in the Web page. The program is loaded on the first computing device after the Web page is received by the first computing device. *See also* claims 33, 38, and 43.

This feature is neither suggested nor disclosed by the cited references.

Remand of the case to the Examiner for a prompt Notice of Allowance is earnestly solicited.

The Notice of Appeal is believed to be timely and no additional fee is believed to be required. However, please credit any overpayment or debit any underpayment to Deposit Account 19-1970 and if an extension is required such extension is hereby petitioned.

Respectfully submitted,
SHERIDAN ROSS P.C.

By: _____
Jason H. Vick
Registration No. 45,285
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: 2-25-02

J:\4366\-41\pre-appealbrief2